Incident Response

// Ransomware

Ransomware strikes a business every 10 seconds.

If your business gets hit, knowing how to respond can minimize the costs and associated downtime. This guide will cover every step a business should take when a ransomware infection occurs.

// What is a Ransomware attack?

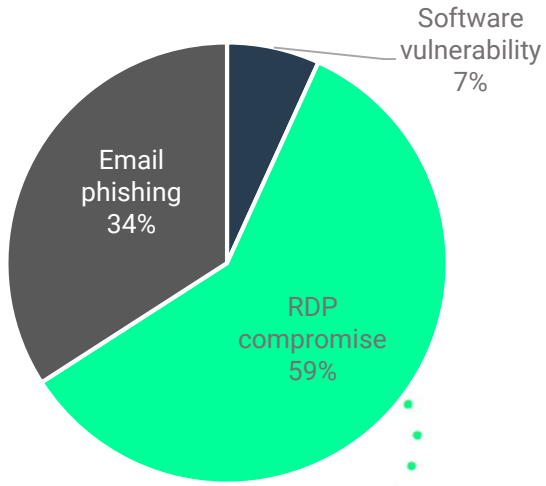
At its most basic level, a Ransomware attack is the use encryption malware to first encrypt data, applications, and hardware, and then subsequently extort the owners of the encrypted assets for a financial payment. After the payment has been made to the Ransomware hackers, a decryption tool or key is provided to the victim, who may then attempt to recover their data.
The ability for ransomware to propagate within a company's network can lead to catastrophic downtime, which can cripple an organization and can often lead to bankruptcy. The cost of downtime is often 10-100x the cost of an individual ransom amount demanded.

// How does Ransomware spread?

The hackers primarily use the following attack vectors to infect a machine: **vulnerable ports, phishing emails, social engineering, unpatched software, compromised websites or advertising and free software downloads**.

Ransomware can encrypt the files on an individual computer or be designed to move through connected drives and devices without outside instruction. When networks are breached by the hacker, the hacker often uses other malware to gain lateral access to different parts of a network to implant ransomware broadly.

Common Attack Vectors for Ransomware



// Join the revolution

// Common Attack Vectors:

Email Phishing: Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity

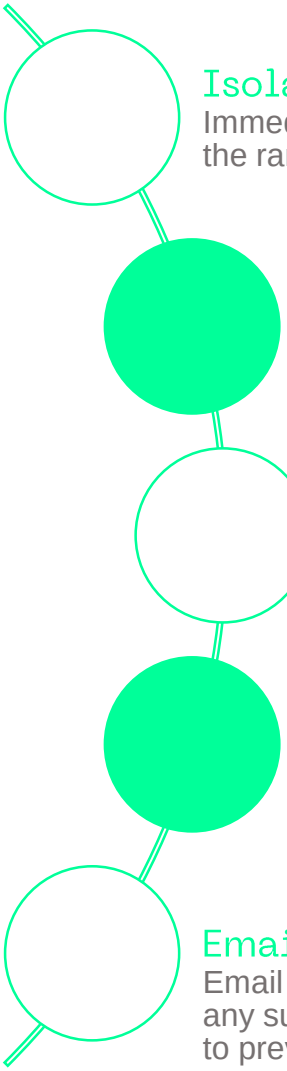
RDP compromise: RDP (Remote Desktop Protocol) is a common protocol used by businesses of all sizes that was first introduced in the 90s. Without proper security, RDP has become a common attack vector as it allows a hacker to sidestep endpoint protection and makes lateral proliferation between partitioned networks

METABASE Q

// We start working immediately

Metabase Q utilizes a combination of people, processes and technology to provide fast results and swift remediation and recovery. When ransomware hits and backups fail, it is a company-wide emergency. We help you focus on your internal recovery, while our professionals handle the specialized process of cyber extortion negotiations and ransomware encrypted data recovery. Let our experts guide your company through a secure, compliant, expedient ransomware recovery.

Our first 2 hours: Our aim is to stop the problem from getting bigger



Isolate Infected Machines

Immediately disconnect infected machines from the network to prevent the ransomware from spreading further

Close RDP Ports

Remote Desktop Protocol is one of the most common attack vectors for ransomware. We will immediately close your ports that are open to the internet and review logs to determine if this was the point of ingress

Change Administrative Credentials

It should be assumed that either current credentials have been compromised or a new set has been created by attacker. If this step is not followed, it could enable the attacker to reinfect your network

Change User Credentials

Domain admin credentials are usually harvested from a subordinate machine of an employee. We force a password change across your entire user base to ensure credentials cannot be elevated

Email Forensics and Anti-Phishing

Email phishing is the other most common attack vector. We will analyse any suspicious inbound emails as well as place preventative measures to prevent your company from being infected again

Following our immediate remediation and initial assessment, we will take a full inventory of what data has been encrypted and business operability. If any critical data was encrypted and backups are unavailable then there is a chance engaging with the hacker and paying the ransom is necessary. Although a last resort, it is widely understood that if data loss is not an option, then negotiating for and paying a ransom is a necessary path to recovery.

// Join the revolution

METABASE Q

// Metabase Q Incident Response

Your organization has been hit by a ransomware attack. This cyber threat has left files locked, applications down, and your critical business functions crippled. How do you respond to this cyber-extortion? Metabase Q is here to help.

Small businesses, municipalities, and Fortune 500s alike have relied on Metabase Q to respond to and recover from ransomware attacks ranging from one to thousands of business systems.

Our targeted ransomware response solutions minimize the impact in terms of costs and business interruption, get you operational, and prevent you from getting hit again.

// If your organization has been hit by ransomware, we can help:

- Contain the incident and stop additional systems from getting infected
- Coordinate a business continuity plan
- Decide whether or not to pay ransom to the threat actors
- Obtain cryptocurrency to acquire keys for decryption
- Reverse engineer attacker-provided decryption utilities to ensure no malicious code exists
- Investigate to identify the attack vector and malicious activity on your network
- Develop and implement a plan for system recovery
- Monitor business systems for reinfection or subsequent attacks
- Develop an ongoing security plan to level up your company's security and prevent future attacks

// Why Metabase Q

- **Subject matter expertise:** Our teams respond to several ransomware attacks a day. Whether facing Bitpaymer, Dharma, Ryuk, or another variant, we leverage aggregated threat intel and battle intelligence to minimize costs and downtime
- **Powerful, Proprietary Ransomware Response Technology:** Our powerful suite of technology-enabled incident response methodologies and solutions are designed to help clients successfully contain and control ransomware-related threats.
- **Responsiveness:** With ransomware, the clock is ticking. We move fast to help our clients contain, investigate, and coordinate the right response to each specific threat.

// Join the revolution

METABASE Q

// Our Anti-Ransomware approach

Just the thought of ransomware is enough to keep CISOs and security teams up at night. Victims are caught in an awful choice between paying a ransom to a criminal who may or may not release their captured network and data, or potentially spending millions of dollars to remove the ransomware on their own

At Metabase Q, we believe preventive security is the best defense. **You do not have to be a victim.**

Critical steps every organization needs to consider. We can help:

1. **Map your attack surface.** You can't protect what you don't know needs to be protected. Metabase Q starts by doing a full internet scan of all of your internet connected devices, including open ports and cloud instances, to create a full digital and automated inventory. We then map your internal surface to understand all connected devices and potential vulnerabilities.
2. **Patch and upgrade your vulnerable devices**. Establishing and maintaining a regular patching and upgrading protocol is just a basic best practice. Unfortunately, far too many organizations simply don't do it.
3. **Update your security systems**. In addition to updating your networked devices, you also need to ensure that all of your security solutions are running their latest updates and you have the maximum protection. Attackers use new techniques everyday. Metabase Q looks for the best possible security solutions to ensure that our customers are always protected.
4. **Segment your network**. Network segmentation ensures that compromised systems and malware are contained to a specific segment of the network. This includes isolating your intellectual property and sequestering the personal identifying information of employees and customers.
5. **Secure your extended network**. Ensure that security solutions deployed on your core network are replicated in your extended network to prevent security gaps. Also take time to review any connections from other organizations (customers, partners, vendors) that touch your network.
6. **Isolate your recovery systems and backup your data**. You need to perform regular data and system backups and, just as critically, store those backups off-network so they are not compromised in the event of a breach.
7. **Run recovery drills**. Regular recovery drills ensure that your backed-up data is readily available, all required resources can be restored and that all systems operate as expected.
8. **Leverage outside experts**. Establish a list of trusted experts and consultants who can be contacted in the event of a compromise to assist you through the recovery process.
9. **Pay attention to ransomware events**. Stay abreast of the latest ransomware news by subscribing to threat intelligence and news feeds, make it a habit for your team to learn how and why systems were compromised, and then apply those lessons to your own environment.
10. **Educate employees**. Rather than being the weakest link in your security chain, your employees need to be your first line of cyber defense.

// Join the revolution

METABASE Q

// Conclusion

- Our incident response services are recognized globally and utilized by small businesses, municipalities, and Fortune 500s alike
- Our teams respond to several ransomware attacks a day. Whether facing Bitpaymer, Dharma, Ryuk, or another variant, we leverage aggregated threat intel and battle intelligence to minimize costs and downtime
- Our powerful suite of technology-enabled incident response methodologies and solutions are designed to help clients successfully contain and control ransomware-related threats.
- We offer the best-in-class managed service provider services and technologies to work with you post incident to ensure you are safe from future attacks

The world has changed. Your approach to cybersecurity needs to as well.

// Our other services

CISO-as-a-Service

We work alongside your team to design and implement processes, architecture and technology whether its designing a move to the cloud, establishing better risk management procedure or building a cybersecurity department from scratch

Security Solutions

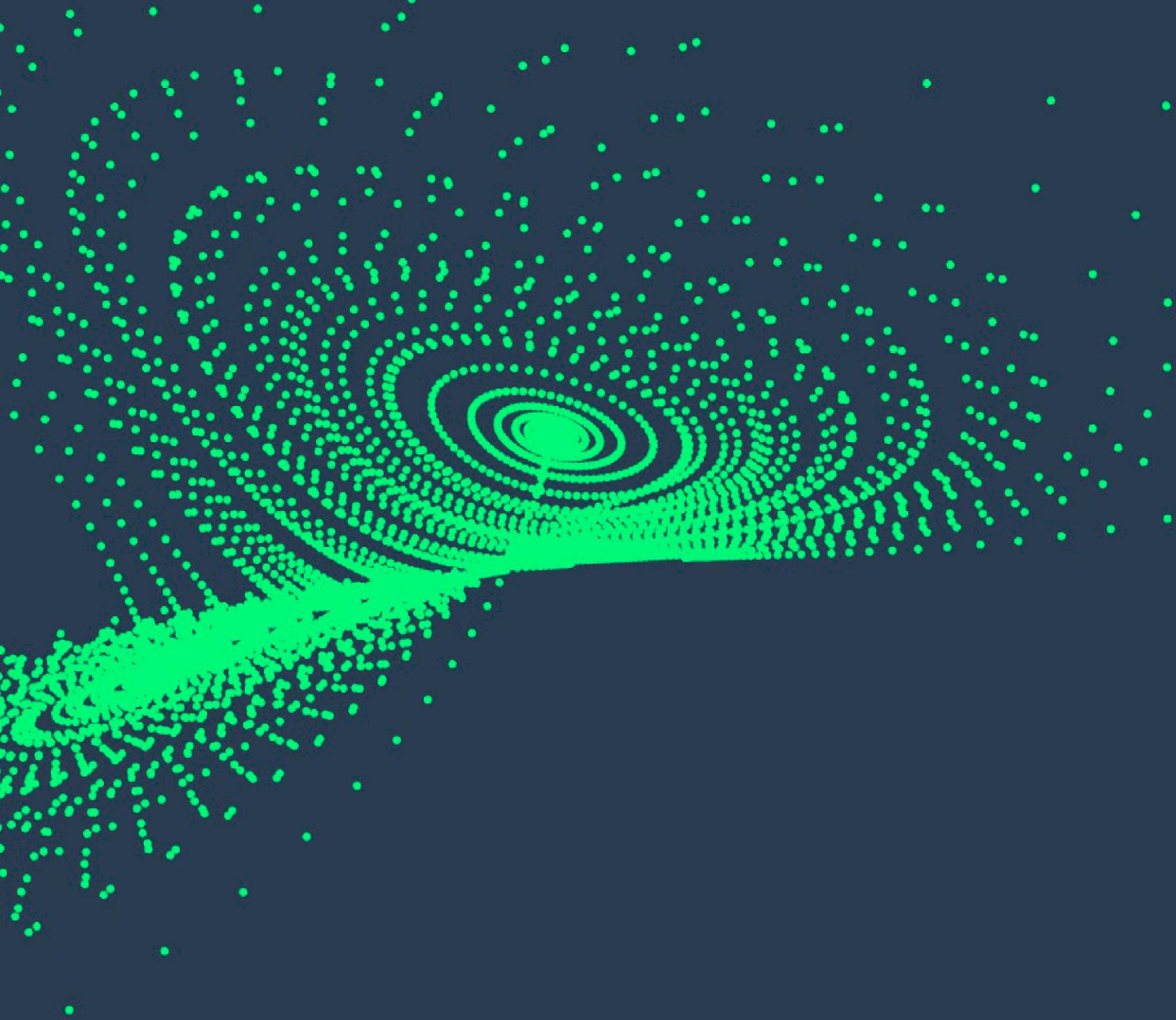
Our product experts draw on their extensive theoretical and practical knowledge to derive maximum benefits from any technologies you are looking to implement or have implemented. We provide training and support for over 40 technologies

Cyber Defense Center

We provide incident response remediation as well as on-going monitoring and threat hunting for your organization

// Join the revolution

METABASE Q



We protect companies that are changing the world.

Join us, join the revolution

contact@metabaseq.com
+52 558 470202

METABASE Q